REMARKS

Reconsideration of the above-identified patent application in view of the remarks following is respectfully requested.

Claims 1-14 and 16-26 are in this case. Claims 1-14 and 16-26 have been rejected under § 103(a).

The claims before the Examiner are directed toward methods, devices and a program-bearing storage device for detecting malicious code in a stream of data traffic input to a gateway of a data network. The gateway is monitored for suspicious data in a portion of the stream of data traffic that is expected to lack executable code. When such suspicious data is detected, an attempt is made to disassemble the suspicious data, preferably starting at every offset in the suspicious data. If the attempt succeeds in producing disassembled executable code, respective threat weights are assigned to the instructions of the disassembled executable code and the threat weights are accumulated to produce an accumulated threat weight. For example, the threat weight could be increased for legal instructions and decreased for illegal instructions.

§ 103(a) Rejections - Radatti et al. '540 in view of Szor '290 and further in view of Voelker et al. '513 and further in view of Schmall

The Examiner has rejected claims 1, 3, 4, 10 and 20 under § 103(a) as being unpatentable over Radatti et al., US Patent No. 7,389,540 (henceforth, "Radatti et al. '540") in view of Szor, US Patent No. 7,293,290 (henceforth, "Szor '290") and further in view of Voelker et al., US Patent No. 6,014,513 (henceforth, "Voelker et al. '513") and further in view of Schmall, "Classification and identification of malicious

code based on heuristic techniques utilizing Meta languages" (PhD thesis, 2003) (henceforth, "Schmall"). The Examiner's rejection is respectfully traversed.

In the Office Action mailed December 24, 2009, the Examiner rejected claims 1, 3, 4, 10 and 20 as unpatentable over Radatti et al. '540 in view of Szor '290 and Schmall. By adding Voelker et al. '513 to the prior art cited against claims 1, 3, 4, 10 and 20, the Examiner has acknowledged that the amendments filed on February 4, 1020 overcome the previously cited prior art.

Voelker et al. '513 teach a computer software tool for identifying code portions and data portions in a binary executable software program whose instructions could start at any byte boundary. One feature of the teachings of Voelker et al. '513 that would prevent one *ordinarily* skilled in the art from thinking of combining those teachings with the other prior art cited by the Examiner to arrive at the invention recited in independent claims 1 and 20 is that Voelker et al. '513 always know in advance that the binary executable software they disassemble definitely includes executable code. For example, the disassembly process of Voelker et al. '513 starts with the determination of a "root set", which is defined in column 5 lines 3-4 as

> ...the set of all addresses in an executable file that are guaranteed to be code or data.

One of these addresses is the entry address. As stated in column 5 lines 25-33,

> For the executable module itself, the entry is the address at which execution begins...Note that this entry address is always known to be for a code component – not data.

By contrast, the entire purpose of the present invention, as stated in claim 1(a) and in claim 20(a)(i), is to detect malicious code in a portion of the stream of data traffic that is expected to lack executable code. It would not occur to one *ordinarily* skilled in the art to seek guidance, on finding malicious code in data that is expected to lack such code, in a prior art document about disassembling a file that is known *a*

priori to *definitely* include executable code. It follows that independent claims 1 and 20 are not at all obvious from the prior art cited by the Examiner.

With independent claim 1 allowable in its present form over the prior art cited by the Examiner, it follows that claims 3, 4 and 10 that depend therefrom also are allowable.

§ 103(a) Rejections - Radatti et al. '540 in view of Szor '290 and further in view of Voelker et al. '513 and further in view of Schmall and further in view of Muttik '780

The Examiner has rejected claims 8, 11, 12, 16-18, 21 and 23-26 under § 103(a) as being unpatentable over Radatti et al. '540 in view of Szor '290 and further in view of Voelker et al. '513 and further in view of Schmall and further in view of Muttik, US Patent No. 6,775,780 (henceforth, Muttik '780"). The Examiner's rejection is respectfully traversed.

The arguments presented above in defense of independent claims 1 and 20 also show, *mutatis mutandis*, that independent claims 11, 16 and 17 are allowable over the prior art cited by the Examiner.

With independent claims 1, 11, 17 and 20 allowable in their present form it follows that claims 8, 12, 18, 21 and 23-26 that depend therefrom also are allowable.

Although claims 23-26 are allowable merely by virtue of depending from claims 1, 11, 17 and 20, Applicant respectfully presents further reasons why these claims are allowable. Claims 23-26 recite the limitation that the attempt to dissemble is initiated at every offset within the suspicious data. The Examiner has cited Voelker et al. '513 as teaching this limitation. In fact, Voelker et al. '513 do not teach this limitation. The disassembly process of Voelker et al. '513 has two phases. In the first

phase, as illustrated in Figures 2-4, the root set is identified and the associated code and data are deconstructed. As stated in column 9 lines 7-9,

> Using the initial root set, the code discovery procedure typically identifies 90% of the text sections of an executable module as code or data.

In the second phase, as stated in column 9 lines 9-11,

> The code discovery procedure now optionally determines new root sets by examining the remaining gaps of unknown bytes in the text sections.

It is this second phase that the Examiner has cited as teaching the limitation of attempting to disassemble starting at every offset. But Voelker et al. '513 in fact teach the *opposite* of what the Examiner seeks to demonstrate. As stated in column 9 lines 11-14,

> This preferred embodiment treats the starting address of each gap as a root, and disassembles the code at that root, using the above described technique. (emphasis added)

In other words, in their second phase, Voelker et al. '513 start disassembly *only* at the starting addresses of the gaps, and *not* at each offset in the gaps.

§ 103(a) Rejections - Radatti et al. '540 in view of Szor '290 and further in view of Voelker et al. '513 and further in view of Schmall and further in view of Muttik '780 and further in view of Shipley '236

The Examiner has rejected claims 2, 6, 7 and 14 under § 103(a) as being unpatentable over Radatti et al. '540 in view of Szor '290 and further in view of Voelker et al. '513 and further in view of Schmall and further in view of Muttik '780 and further in view of Shipley, US Patent No. 6,119,236. The Examiner's rejection is respectfully traversed.

It is demonstrated above that independent claims 1 and 11 are allowable in their present form. It follows that claims 2, 6, 7 and 14 that depend therefrom also are allowable.

§ 103(a) Rejections - Radatti et al. '540 in view of Szor '290 and further in view of Voelker et al. '513 and further in view of Schmall and further in view of Muttik '780 and further in view of Made '076

The Examiner has rejected claims 5, 9, 13, 19 and 22 under § 103(a) as being unpatentable over Radatti et al. '540 in view of Szor '290 and further in view of Voelker et al. '513 and further in view of Schmall and further in view of Muttik '780 and further in view of Made, US Patent Application Publication No. 2002/0056076. The Examiner's rejection is respectfully traversed.

It is demonstrated above that independent claims 1, 11, 17 and 20 are allowable in their present form. It follows that claims 5, 9, 13, 19 and 22 that depend therefrom also are allowable.

In view of the above remarks it is respectfully submitted that independent claims 1, 11, 16, 17 and 20, and hence dependent claims 2-10, 12-14, 18, 19 and 21-26 are in condition for allowance. Prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,

Mark M. Friedman
Attorney for Applicant
Registration No. 33,883
Dr. Mark Friedman Ltd.
Moshe Aviv Tower, 54th Floor
7 Jabotinsky Street
Ramat Gan 52520 ISRAEL
Tel: 972-3-6114100
Fax: 972-3-6114101
Email: patents@friedpat.com

Date: June 7, 2010